Smussenko Diana Alexandrovna
Student
Ural Federal University
Russia, Ekaterinburg
Academic supervisor: Gubina Dilyara Ilshatovna

CYBER KILL CHAIN

Abstract. *The article is devoted to the study of the CKC model. The article discusses the terminology of the SCS model and its history. The steps of the model and their features are also presented. A detailed analysis of each stage was made. Based on the study, a model diagram was created for simplified understanding.*

Keywords: *Cyber Kill Chain, model, framework, preventing cyber-attacks, steps of attacks, features of steps.*

Смусенко Диана Александровна
Студент
Уральский федеральный университет имени первого
Президента России Б.Н. Ельцина
Россия, г. Екатеринбург
Научный руководитель: Губина Диляра Ильшатовна

CYBER KILL CHAIN

Аннотация. *Статья посвящена изучению модели Cyber Kill Chain (CKC). В статье рассматриваются терминология модели СКС и ее история. Также представлены этапы модели и их особенности. Произведен детальный анализ каждого этапа. На основе проведенного исследования была создана схема модели для упрощенного понимания.*

Ключевые слова: *Cyber Kill Chain, модель, фреймворк, предотвращение кибератак, этапы атак, особенности этапов.*

The term «kill chain» was originally used as a military concept. The Cyber Kill Chain (CKC) was proposed in 2011 by Martin Lockheed and has since been widely used in the industry to model intrusion attempts by alleged attackers. The developed framework «Cyber Kill Chain» is a part of the Intelligence Driven Defense model and is used to detect and prevent cyber-attacks.

This model defines what attackers need to do in order to achieve their goals by attacking the network, extracting data, and maintaining a presence in the organization. Thanks to this model, we know that blocking hackers at any stage breaks the entire chain of attack. Again, to be successful, hackers have to go through all the stages, and, in turn, we, the defending side, just need to block them at any stage to achieve at least minimal success.

To counter attackers, Lockheed Martin introduced the CKC model with the concept of advanced and persistent threats, which explains the «threat» using 6 stages, starting with intelligence and ending with actions on the target. Later, based on these studies, the model was expanded to 7 stages, which are still used today.

Steps of attacks

The Cyber Kill Chain model indicates that hackers must always go through the following main stages to carry out their atrocities:

Stage 1. Reconnaissance

At this stage, the main goal of the attacker is to find information about the target.

Stage 2. Weaponization

During the arming stage, attackers arm their malware, which they use to penetrate the target and bypass its security systems. They use a range of methods, from masking malware that looks like regular data, such as PDF and Microsoft Office documents, to antivirus software.

Stage 3. Delivery

This stage is one of the most important, because it does not matter how good and effective a malicious program is, without its delivery to the victim, it is useless. Therefore, delivery can be performed using a variety of methods, which makes attackers more likely to deliver a malicious application.

Stage 4. Exploitation

After delivery to the user's computer or device, the required (malicious) content is deployed and installed in the environment. This usually happens when using a known vulnerability that previously had a patch available. Further implementation of Crimeware-as-a-Service (CaaS) reduces the amount of trouble for attackers at this stage.

Stage 5. Installation

During this process, the attacker gains privileges on the victim's device, increasing their capabilities, and opening previously closed opportunities for them.

Stage 6. Command and Control (C&C, or C2)

After installing malicious software on the victim's computer, it is time for attackers to start manipulating their victims' systems. At this stage, hackers begin to control the victim's assets using management methods (usually remote) such as DNS, Internet control Message Protocol (ICMP), websites, and social networks.

Stage 7. Actions on Objective

In the final part of the chain, attackers collect the necessary data, send it through secure channels, and disable the target's IT assets while they are located.

Features of steps

Reconnaissance

Reconnaissance requires gathering as much information as possible. From any distance and of any importance, lists with email addresses, interception of messages, research of social networks, checking the openness of ports, for the subsequent introduction of malicious applications into the system. Information is collected about possible vulnerabilities that may be exploited in the future. Information about the apps

you use is also collected. Information gathering is usually used to determine the best tool for an attack (a single tool, a system of tools, or a worm, as well as various other methods of penetration) and then penetrate the target with minimal effort for the most effective and guaranteed defeat of the target.

This stage has several drawbacks, the most obvious one is that the target may expect to be tracked and collect information about itself, and therefore may use secure channels or have false data used as a screen.

Weaponization

Based on the information gathered during the investigation and the study of the technical part of the victim, the mechanisms of penetration and capture are selected. Among them, 5 main weapon techniques are used including: embedding commands using a script, delivering a useful diversifying load, sabotage (hidden attacks) of the file access structure, possible diversification using encryption, and the use of various methods of evading detection (based on time, data, code, and network).

Delivery

Delivery can be compared to fishing. The attacker throws the bait and waits for the target to catch it, or the attacker personally implements a malicious application of the target. The baited method is implemented using malicious e-mail distribution or sending an infected file using social engineering. If attackers deliver a malicious application, they can do so using a prepared USB storage device.

The main disadvantage of this method is that the target can be prepared and train personnel for the interaction of a social hacker, can protect USB connectors and perform data transfer inside the network at the local level, without having access to the Internet.

Exploitation

The peculiarity of exploitation is that after delivering a malicious software to the victim's system, the attacker needs to run this software. This is usually done by exploiting vulnerabilities in the target environment using a set of exploits or running a target exploit. The set of exploits refers to the tools of hacker software. This software

is used to scan the system for vulnerabilities (software without a patch) and then use these vulnerabilities. A clear example is Adobe Flash without a patch or Microsoft SilverLight, such a vulnerability was exploited by malicious software such as CrypWall, TeslaCrypt, Crilock, and Waltrix. A target exploit differs from an exploit kit in that it targets a specific target and a specific device. And it is an exploit for a small number of attacks on a single company or a small number of people. An example of such an exploit is the Petya ransomware, later announced as Wiper.

Installation

To do this, an attacker can use a variety of techniques, starting with simple Remote access Trojans, ending with the creation of permanent backdoors that allow the attacker to enter the system, even if the main application is deleted, the attacker can re-upload data to the system for subsequent manipulations with the target.

This stage has several possible difficulties for the attacker. The target system may have a powerful firewall and a good team of information security specialists who can isolate the infected system at the right time and neutralize the malicious software.

Command and Control

There are many important aspects to a thing like C2. If there is a network for an organization, the program will try to spread within that network. The next step is to encrypt the program itself in order to become invisible to antivirus software. The program also performs a scan to find the best distribution paths. Next, let's look at the controls using ransomware as an example. The program encrypts the victim's data and sends a notification about the need to pay money to restore files. After the program receives confirmation, it sends the public key to decrypt the files. An example of such a program is the aforementioned program, Petya.

Actions on Objective

Next, the attacker takes steps to expand its presence within the organization and then extract data. The attacker spreads his malicious applications throughout the victim's network and expands his influence.

The main feature of Cyber Kill Chain is that it is circular, not linear. As soon as a hacker has entered the network, he starts this chain again inside the network, performing additional intelligence and performing horizontal promotion inside Your network.

In addition, it should be borne in mind that although the methodology is the same, hackers will use different methods for internal chain stages when they are inside the network than when they are outside the network. In fact, after a hacker enters the network, he becomes an insider.

General scheme of the Cyber Kill Chain model

Based on the collected information, we can create a diagram of each stage and the processes that occur in them. This diagram will greatly simplify the understanding of all the processes that occur in CKC (figure 1).

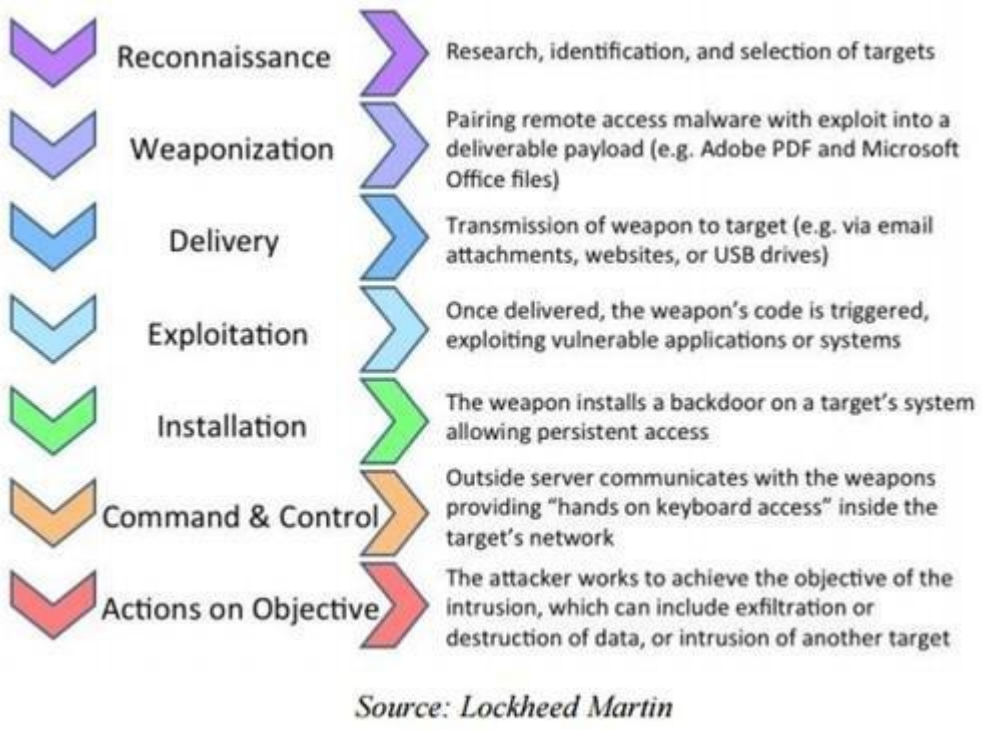

Fig. 1 – Scheme of the Cyber Kill Chain by Lockheed Martin

REFERENCES

1. The Cyber Kill Chain. – 2020. – [Text: electronic]. – URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (Reference date 07.12.2020).

2. What is Cyber-Kill Chain and why we need to mind its defense strategies? – 2017. – [Text: electronic]. – URL: https://habr.com/ru/company/panda/blog/327488/ (Reference date 07.12.2020).

3. Modified cyber kill chain model for multimedia service environments. – 2018. – [Text: electronic]. – URL: https://www.scopus.com (Reference date 09.12.2020).

4. A Cyber-Kill-Chain based taxonomy of crypto-ransomware features – 2019. – [Text: electronic]. – URL: https://www.scopus.com (Reference date 10.12.2020).